REMARKS

This communication is a full and timely response to the aforementioned Office Action dated November 19, 2009. By this communication, 34-49 are added. Claims 1-12, 17-20, 22-24 and 28, 29 and 31-33 are not amended and remain in the application. Therefore, claims 1-12, 17-20, 22-24, 28, 29 and 31-49 are pending in the application. Claims 1, 7, 17, 31, 38 and 44 are independent.

Reconsideration of the application and withdrawal of the rejections of the claims are respectfully requested in view of the foregoing amendments and the following remarks.

I. Interview

Applicants thank the Examiner for kindly conducting a personal interview with Applicants' undersigned representative on March 9, 2010. During the interview, Applicants' representative discussed exemplary embodiments of the present that provide support for the features of the claimed invention. In addition, Applicants' representative discussed several reasons why claims 1, 7, 17 and 31 are patentable over Smetters (U.S. Patent Application Publication No. 2004/0088548) and Benussi et al. (U.S. Patent Application Publication No. 2001/0044898, hereinafter "Benussi"). Applicants' representative also discussed distinguishing features of proposed new claims 34-45. Proposed new claims 34-45 as discussed during the interview are presented herein as new claims 38-49, respectively.

Distinguishing features of the claimed invention are summarized below.

II. Rejections Under 35 U.S.C. § 103

Claims 1, 4, 5, 7, 10, 12, 17, 20, 22-24 and 31 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Benussi. This rejection is respectfully traversed for at least the following reasons. Furthermore, Applicants respectfully submit that this rejection is inapplicable to new claims 34-49.

(A) Exemplary Embodiments Supporting Claimed Invention

An exemplary embodiment of the present invention provides a communication system in which an image processing apparatus 100 and a client 200 communicate with each other through a network 300 (see Figure 1).

As shown in Figure 2, for example, the image processing apparatus 100 includes a first storage device 118, is configured to create a root certificate 126. The root certificate 126 includes a public key paired with a private key and is signed with the private key. Accordingly, the image processing apparatus 100 comprises a root certificate creator which creates the root certificate 126, which includes a public key paired with a private key, and which is signed with the private key.

The image processing apparatus 100 also includes a second certificate creator 124 which creates a second certificate 128. The second certificate creator 124 creates the second certificate 128 when a connection for communication with the image processing apparatus 100 is requested by the client 200. According to an exemplary embodiment, the connection for communication requested by the client 200 is a request for encrypted communication between the image processing apparatus 100 and the client 200. See, for example, paragraphs [0008], [0028] and [0048] on pages 5, 6, 11, 12 and 19-21 of the original specification.

The second certificate 128 designates the root certificate 126 as a certificate authority at a higher level and is signed with the private key used to sign the root certificate 126. According to an exemplary embodiment, the second certificate 128 transmitted to the client 200 after the root certificate 126 is installed in the client 200 includes path information to the root certificate. For example, the path information included in the second certificate 128 can include information identifying an issuer of the root certificate 126 (e.g., the root certificate creator in the image processing apparatus 100), to, for example, designate the root certificate 126 as a certificate authority at a higher level. The image processing apparatus 100 comprises a communication device 106 which transmits the second certificate 128 created by the certificate creator 124 to the client 200 (see Figure 2).

With reference to Figure 3, for example, the client 200 includes a storage device 214 which has stored therein, before the connection for communication is requested to the image processing apparatus 100, the root certificate 222 (126)

created by the root certificate creator 126 of the image processing apparatus 100. The client 200 also comprises a verifier which verifies the signature of the second certificate 128 received from the image processing apparatus 100 with the root certificate 222 (126) already stored in the storage device 214.

Accordingly, the disclosed embodiment provides that the root certificate 222 (126) created by the root certificate creator of the image processing apparatus 100 is also stored in the second storage device 214 of the client 200 before the client 200 requests a connection for communication to the image processing apparatus 100. Therefore, the root certificate 222 (126) is stored in the client 200 prior to initiation of communication between the image processing apparatus 100 and the client 200. Furthermore, the disclosed embodiment provides that the image processing apparatus 100 creates the second certificate 128, which designates the root certificate 222 (126) as a certificate authority at a higher level and which is signed with the private key used to sign the root certificate 222 (126), when the client 200 requests the image processing apparatus 100 for a connection for communication therebetween (see, for example, paragraph [0028] on pages 11 and 12 of the specification). Accordingly, the disclosed embodiment provides that the root certificate 222 (126) created by the image processing apparatus 100 is installed in the client 200 prior to an initiation of communication between the client 200 and image processing apparatus 100, and then, after the client 200 requests a connection for communication to the image processing apparatus 100, the image processing apparatus 100 creates and sends the second certificate 128 to the client 200.

The above-described exemplary embodiment provides an advantageous aspect of enabling the image processing apparatus 100 and the client 200 to securely communicate with each other through the network 300, without requiring either the image processing apparatus 100 or the client 200 to purchase an electronic certificate from an authority outside the network, such as a third-party certificate authority (CA). This is achieved because the root certificate 126 created by the image processing apparatus 100 is also stored in the second storage device 214 of the client 200, prior to an initiation of communication between the image processing apparatus 100 and the client 200. After the client 200 requests a

connection for communication to the image processing apparatus 100 and receives the second certificate 128 from the image processing apparatus 100, the verifier of the client 200 can then verify the signature of the received second certificate 128 with the root certificate 222 (126) that is already stored in the storage device 214 of the client 200. Consequently, the client 200 does not require a certificate issued by a third-party CA or a CA outside the network to verify the second certificate 128 received from the image processing apparatus 100.

(B) Independent Claims 1, 7, 17 and 31

Independent claims 1, 7, 17 and 31 each recite various features of the above-described exemplary embodiment.

Claim 1 recites a communication system in which an image processing apparatus and a client communicate data with each other through a network. Claim 1 recites that the image processing apparatus comprises a root certificate creator which creates a root certificate including a public key paired with a private key and signed with the private key. In addition, claim 1 recites that the device comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate. Claim 1 also recites that the client comprises a storage device which has stored therein, before the connection for communication is requested to the image processing apparatus, the root certificate created by the root certificate creator of the image processing apparatus.

Claim 7 recites a communication method for a communication system in which an image processing apparatus and a client communicate data with each other through a network, wherein the image processing apparatus creates a root certificate including a public key paired with a private key and being signed with the private key. The method of claim 7 also comprises the client installing the root certificate which is created by the image processing apparatus, prior to the client requesting a connection for communication to the image processing apparatus. In addition, the method of claim 7 includes the device creating, when a connection for communication is requested by the client, a second certificate designating the root

certificate as a certificate authority at a higher level and being singed with the private key used to sign the root certificate when data is sent to the client.

Claim 17 recites an image processing apparatus to be used in a communication system in which the image processing apparatus and a client communicate with each other through a network, the image processing apparatus sends information to the client, and the client uses the information to communicate with the image processing apparatus . The image processing apparatus of claim 17 comprises a root certificate creator which creates a root certificate including a pair of a public key and a private key and being signed with the private key. In addition, the image processing apparatus of claim 17 comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to the sign the root certificate. The image processing apparatus of claim 17 also comprises an interface which sends the root certificate to the client before the connection for communication is requested, and sends, after the root certificate created by the root certificate creator is installed in the client, the second certificate for verification of the information sent from the image processing apparatus.

Claim 31 recites a computer-readable recording medium having a computer program recorded thereon that causes a computing device to perform operations of storing a pair of a public key and a private key, creating a root certificate signed with the private key, and sending information and the root certificate created by the computing device and including the public key to the client, before a request for communication is requested by the client. In addition, claim 31 recites that the computer program causes the computing device to perform an operation of creating, when the connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate.

Accordingly, independent claims 1, 7, 17 and 31 each recite that the image processing apparatus (computing device) (1) creates a root certificate that is stored and/or installed in the client before a request for communication is requested by the client, and (2) creates a second certificate, which designates the root certificate as a

certificate authority at a higher level and which is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client.

Applicant respectfully submits that the applied references do not disclose or suggest the above-described features (1) and (2) of independent claims 1, 7, 17 and 31 for at least the following reasons.

(C) Applied References Do Not Disclose or Suggest a Second Certificate Signed With a Private Key Used to Sign a Root Certificate

The Office asserted that the feature of a second certificate, which designates a root certificate as a certificate authority at a higher level, and which is signed with a private key is disclosed in Smetters. This assertion is contrary to the *actual* disclosure of Smetters. In striving to arrive at the subject matter of claims 1, 7, 17 and 31, the Office mischaracterized the disclosure of Smetters as disclosing something it does not. In particular, based on its unsupportable interpretation that Smetters discloses the "creation of two certificates in the same manner," the Office mischaracterized the disclosure of Smetters in interpreting that the second certificate is signed with the private key used to sign the first certificate. The *actual* disclosure of Smetters specifically refutes this interpretation.

Smetters discloses an opposite configuration to that of claims 1, 7, 17 and 31. The Office alleges that Smetters disclose a technique of signing a second certificate with the same private key used to sign the root certificate. In striving to arrive at the subject matter of claims 1, 7, 17 and 31, the Office disregarded the intermediate steps of Smetters that occur between (A) the first device 12(1) generating a first certificate 30 (paragraph [0025] of Smetters) and (B) the first device 12(1) generating and sending a second certificate 40, together with the first certificate 30, to the second device 12(2) (paragraph [0031]). Smetters discloses two different techniques of transitioning from point (A) to point (B). In particular, Smetters discloses that (1) the first laptop 12(1) signs the second certificate 40 with the public key that is generated by the first device 12(1), or the first device 12(1) signs the second certificate 40 with the public key that is transmitted to the first device 12(1) by

the second device 12(2). In either case, the first device 12(1) signs the second certificate 40 with a public key.

In view of the Office's misrepresentation of the disclosure of Smetters in striving to arrive at the subject matter of claims 1, 7, 17 and 31, the *actual disclosure* of Smetters is summarized below to illustrate how the *actual disclosure* of Smetters refutes the Office's interpretation. The two different techniques of transitioning from point (A) and point (B) are also discussed below, even though the Office believes it can disregard them.

(1) Generation of Root Certificate 30

Smetters discloses a system 10 for creating a shared resource space 20 containing resources 22, 24 to be shared among a first device 12(1) and a second device 12(2) (see Figures 1 and 3). The first device 12(1), which has access to the resources 22, 24, generates a root key pair to be used for authentication and encryption when providing the second device 12(2) with access to the shared space 20 (see paragraph [0025], step 100 in Figure 2, and step 120 in Figure 4). In order to share access to the space 20, the first device 12(1) then "generates a first certificate 30 for the new space 20, and digitally signs the [root] certificate 30" (see paragraph [0025], step 100 in Figure 2, and step 130 in Figure 4) (emphasis added). The Office has interpreted the above-quoted section of Smetters as disclosing that the first device 12(1) signing the root certificate with a private key. Even with this interpretation, Smetters does not disclose or suggest that the first device 12(1) creates a second certificate 40 and signs the second certificate 40 with the private key used to sign the first certificate 30.

(2) Establishing Secure Communication

After the first device 12(1) has generated the first certificate 30, the first device 12(1) then transmits range-limited signals to the second device 12(2) to establish a secure communication channel between each other (see paragraph [0028], step 200 in Figure 2). Paragraph [0028] of Smetters also discloses that the second device 12(2) may initially send the range-limited signals to initiate the establishment of a secure communication channel with the first device 12(1).

Smetters discloses that the range-limited signal transmitted from the first device 12(1) includes a public key to secure the communication channel between the first and second devices 12(1), 12(2) (see paragraph [0029]). Once a secure communication channel between the first device 12(1) and second device 12(2) has been established, Smetters discloses that the first device 12(1) then sends an invitation message to the second device 12(2) that invites the second device 12(2) to accept access to the shared space 20 (see paragraph [0030], and step 300 in Figure 2).

(3) Decision by Second Device 12(2) Concerning Which Public Key to Use

Smetters discloses that the second device 12(2) then decides whether to use a particular public key (i.e., the public key included in the range-limited signal from the first device 12(1) or a public key generated by the second device 12(2)) to communicate with the first device 12(1) (see paragraph [0032] and step 510 in Figure 6). The two different techniques are discussed in sections 3A and 3B below.

(3A) Second Device 12(2) Decides to Use Other Public Key

If the second device 12(2) decides to use a particular public key instead of the public key included in the range-limited signal (section (2) above) from the first device 12(1), the second device 12(2) transmits the desired public key to the first device 12(1) (see paragraph [0032] and step 520 in Figure 6). If the second device 12(2) decides to use a particular public key for encryption instead of the public key generated by the first device 12(1), it is not necessary for the first device 12(1) to transmit the corresponding private key to the second device 12(2), because the corresponding private key 12(2) is already in the possession of the second device 12(2).

(3B) Second Device 12(2) Decides to Use Public Key Generated By First Device 12(1)

On the other hand, if the second device 12(2) decides to use the public key generated by the first device 12(1) and included in the range-limited signal, the first device 12(1) generates a pair of a public key and a private key, and sends the

private key of the generated key pair to the second device 12(2) (see paragraph [0033], and steps 530 and 540 in Figure 6). If the second device 12(2) desires to use the public key generated by the first device 12(1), the first device 12(1) must therefore send the corresponding private key to the second device 12(2), or else the second device 12(2) could not decrypt a communication that was encrypted with the public key generated by the first device 12(1).

According to principles of cryptography, the first device 12(1) would not sign the second certificate 40 with the private key that the first device 12(1) sent to the second device 12(2), because the private key would be susceptible to interception.

(4) Generation of Second Certificate 40

After the second device 12(2) decides which public key to use (3(A) or 3(B)), the first device 12(1) then creates a second certificate 40 using either the public key sent from the second device 12(2) or the public key of the key pair generated by the first device 12(1) (see paragraph [0034], step 500 in Figure 2, and step 550 in Figure 6). The second certificate 40 designates the second device 12(2) as a member of the shared space 20 (see paragraphs [0031] and [0034], step 500 in Figure 2, and step 550 in Figure 6). Smetters discloses that the first device 12(1) sends both the first certificate 30 and the second certificate 40 to the second device 12(2) at the same time as a certificate chain (see paragraph [0035]).

The different techniques used to generate the second certificate respectively correspond to whether (3A) the second device 12(2) decides to use a different public key, or (3B) the second device 12(1) decides to use the public key generated by the first device 12(1). The two different techniques of Smetters are disclosed in sections 4A and 4B below.

(4A) First Device Signs Second Certificate 40 With Public Key Sent By Second Device 12(2)

This technique of Smetters is illustrated in Figure 6 with respect to step 520. In this technique (4A), the second device 12(2) retains the private key corresponding to the public key transmitted to the first device 12(1), because the first device 12(1) signs the second certificate 40 with the public key and the second device 12(2) must

therefore possess the corresponding private key in order to decrypt the second certificate 40. In public-private key cryptography, encrypted data can only be decrypted by using one key of a key pair, when the other key of the key pair was used to encrypt the key pair. Therefore, in view of the disclosure of Smetters that the second device 12(2) sends the public key to be used in signing the second certificate 40 to the first device 12(1), the second device 12(2) must retain possession of the corresponding private key in order to decrypt the second certificate 40 sent from the first device 12(1).

Furthermore, Applicant respectfully submits that it is not possible for the first device 12(1) to sign the second certificate 40 with a private key corresponding to the public key transmitted from the second device 12(2), because Smetters does not disclose or suggest that the second device 12(2) transmits the private key corresponding to the public key that was transmitted from the second device 12(2). Moreover, such an interpretation would be contradictory to the principles of public-private key cryptography.

Therefore, according to the first technique (4A) in which the second device 12(2) transmits a public key to the first device 12(1) and the first device 12(1) signs the second certificate 40 with the public key received from the second device 12(2), the first device 12(1) does not sign the second certificate 40 with a private key corresponding to the public key transmitted from the second device 12(2).

Furthermore, the first device 12(1) does not sign the second certificate 40 with the private key used to sign the first certificate 30. Such a construction would not be possible according to the first technique (4A) of Smetters, because the first certificate 30 is generated by the first device 12(1) after the first device 12(1) has generated a root key pair (see paragraph [0025]), and the second certificate 40 is generated by the first device 12(1) using the public key transmitted from the second device 12(2). A public or private key of one root key pair does not correspond to a public or private key of another root key pair. Accordingly, it would not be possible according to the first technique (4A) of Smetters for the first device 12(1) to sign the second certificate 40 using the same private key used to sign the first certificate 30, because different key pairs are used for generating the first certificate 30 and the second certificate 40.

(4B) First Device 12(1) Signs Second Certificate 40 With Public Key Generated By First Device 12(1)

The second technique of Smetters is illustrated in Figure 6 with respect to steps 530 and 540. In this technique, the first device 12(1) generates a public and private key pair (step 530), and sends the private key corresponding to the public key pair to the second device 12(2) (see paragraph [0033]). The first device 12(1) must send the private key corresponding to the public key that is used to sign the second certificate 40, because the second device 12(2) would not be able to decrypt the second certificate 40 unless it was provided with the private key. The disclosure in paragraph [0033] further emphasizes that the first device 12(1) does not sign the second certificate 40 with the private key corresponding to the public key, because sending the private key of the newly generated key pair to the second device 12(2) would not, in any way, permit the second device 12(2) to decrypt the second certificate 40, if the second certificate 40 was hypothetically signed with the private key of the newly generated key pair. If the second certificate 40 was hypothetically signed with the private key of the newly generated key pair, then the first device 12(1) would need to send the public key of the newly generated key pair, so that the second device 12(2) could decrypt the second certificate 40. However, Smetters discloses the opposite technique in which the first device 12(1) transmits the private key to the second device 12(2), because the second certificate 40 is signed with the public key of the key pair that is newly generated by the first device 12(1).

Therefore, according to the second technique (4B) of Smetters in which the first device 12(1) generates a new key pair and transmits the private key of the newly generated key pair to the second device 12(2), Smetters does not disclose or suggest that the second certificate 40 is signed with a private key.

Furthermore, the first device 12(1) does not sign the second certificate 40 with the private key used to sign the first certificate 30. Such a construction is contradictory to the disclosure of Smetters. In particular, Smetters discloses that when the second device 12(2) elects to have the first device 12(1) use a public key generated by the first device 12(1) to generate the second certificate 40, the first device 12(1) generates a new key pair (see paragraph [0033, and step 530 in Figure 6]). The new key pair generated by the first device 12(1) to generate the second

certificate 40 in step 530 of Figure 6 (corresponding to step 500 in Figure 2) is different from the key pair generated by the first device 12(1) to generate the first certificate 30 in step 120 of Figure 4 (corresponding to step 100 in Figure 2), because these key pairs are generated at different stages within the resource management process of Figure 2 and therefore are different key pairs. A public or private key of one root key pair does not correspond to a public or private key of another root key pair. Consequently, Smetters does not disclose or suggest that the first device 12(1) signs the second certificate 40 with the private key used to sign the first certificate 30.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that no disclosure of Smetters, even given the broadest reasonable interpretation, supports the Office's assertion that Smetters somehow discloses that the second certificate 40 is signed with a private key used to sign the root certificate. The Office's assertion is factually erroneous and is specifically refuted by the disclosure of Smetters.

Therefore, Applicant respectfully submits that that Smetters does not disclose or suggest that the second certificate 40 (or any other subordinate member certificate) is signed with the private key used to sign the first certificate 30.

Consequently, Smetters does not disclose or suggest that the first device 12(1) creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Benussi also does not disclose or suggest these features of claims 1, 7, 17 and 31. On the contrary, Benussi discloses that a root certificate ("Root CA") of a CSS (communication service system) 20 is signed with a private key of the CSS 20, and the root certificate of CSS 20 is pre-installed in the CB (connectivity box) 11 for the initial configuration of the CB 11 (see paragraph [0214], lines 24-30 and 51-55, and Figure 1).

However, similar to Smetters, Benussi does not disclose or suggest that a second certificate, which designates the Root CA of the CSS 20 as a certificate authority at a higher level, is signed with the private key of the CSS 20 used to sign

the Root CA. On the contrary, with reference to paragraph [0214], Benussi discloses that a CB certificate is downloaded to the CB 11 as a pre-installed parameter 190. Even if the Office is to interpret the CB certificate as being signed, the CB certificate is not in any way signed with the same private key used to sign the Root CA. There is no disclosure in Benussi to remotely support this interpretation.

Therefore, neither Smetters nor Benussi disclose or suggest an image processing apparatus that creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

(D) Applied References Do Not Disclose or Suggest that a Root Certificate is Installed in a Client Prior to a Request for Communication from the Client

Smetters discloses that the first device 12(1), which has access to the resources 22, 24, generates a root key pair to be used for authentication and encryption when providing the device 12(2) with access to the shared space 20 (see paragraph [0025], step 100 in Figure 2, and step 120 in Figure 4). In order to share access to the space 20, the first device 12(1) generates a first certificate 30 for the new space 20 (see paragraph [0025], step 100 in Figure 2, and step 130 in Figure 4).

Smetters discloses that the first device 12(1) then generates a second certificate 40 to be transmitted to a second device 12(2). As discussed above, the first device 12(1) generates the second certificate using either (i) a public key sent from the second device 12(2) to the first device 12(1), or (ii) a public key generated by the first device 12(1) (see paragraph [0034], and step 550 in Figure 6).

Smetters discloses that the first device 12(1) then sends both the root certificate 30 and the second certificate 40 to the second device 12(2). In particular, the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device at the same time after the second certificate 40 is created. The second device 12(2) then stores the received root certificate 30 and second certificate 40 in a memory thereof (see paragraph [0035] and step 600 in Figure 2).

Accordingly, as acknowledged by the Office, Smetters does not disclose or suggest that the second certificate 40 created by the first device 12(1) is stored or installed in the second device 12(2) before the second device 12(2) requests communication to the first device 12(1).

In an attempt to arrive at this feature, the Office applied Benussi. However, Benussi also does not disclose or suggest feature (1) of claims 1, 7, 17 and 31.

On the contrary, Benussi discloses that "the public key of the Root CA is pre-installed in each CB [connectivity box] as the 'Certificate for Root CA' of [pre-installed] parameters 190" (see paragraph [0214], lines 53-55) (emphasis added). Benussi discloses that the Root CA is the "root certificate authority" (see paragraph [0214], lines 26-27).

Accordingly, Benussi discloses that the public key of the Root CA, not the Root CA, is preinstalled in the CB. Furthermore, Benussi discloses that the CB receives the public key of the Root CA from the CSS (communication service system). However, the CSS does not create the Root CA.

Consequently, Benussi does not disclose or suggest that the CB has stored or installed therein a Root CA which is created by the CSS, before a connection for communication is requested to the CSS by the CB.

Therefore, Smetters and Benussi, either individually or in combination, do not disclose or suggest an image processing apparatus (computing device) that creates a root certificate that is stored and/or installed in the client before a request for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Accordingly, for at least the foregoing reasons, Applicants respectfully submit that claims 1, 7, 17 and 31 are patentable over Smetters and Benussi, since Smetters and Benussi, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 7, 17 and 31.

(E) New Claims 38 and 44

New claims 38 and 44 each recite an image forming apparatus which communicates with a client through a network. The image forming apparatus of new claims 38 and 44 comprise a communication device which transmits a first certificate stored by a storage device of the image forming apparatus to a client. New claims

38 and 44 each recite that the communication device is configured to transmit a second certificate, which includes path information to the first certificate stored in the image forming apparatus, to the client when a connection for encrypted communication is requested by the client after the first certificate stored in the image forming apparatus is installed in the client.

Smetters does not disclose or suggest that the first device 12(1) transmits the second certificate 40 to the second device 12(2) when a connection for encrypted communication is requested by the second device after the first certificate 30 is installed in the second device 12(2). On the contrary, Smetters discloses that the first device 12(1) transmits the first and second certificates 30, 40 at the same time. Therefore, it is not possible for the second certificate 40 of Smetters to be installed in the second device 12(2) when the second device 12(2) requests communication from the first device 12(1).

Furthermore, Smetters also does not disclose or suggest that second certificate 40 (together with the first certificate 30) is transmitted to the second device 12(2) when a request for encrypted communication is requested by the client. On the contrary, as discussed above, the first device 12(1) and the second device 12(2) exchange range-limited signals prior to the exchange of any certificates 30, 40 (see paragraph [0029]). Smetters does not disclose or suggest that the second device 12(2) requests a connection for encrypted communication to receive the second certificate 40, after the first device 12(1) and second device 12(2) have authenticated each other through the exchange of the range-limited signals. On the contrary, once the first device 12(1) and second device 12(2) have authenticated each via the range-limited signals, the second device 12(2) does not issue a request for encrypted communication.

Benussi also does not disclose or suggest the features of claims 38 and 44. Benussi discloses that after a CB has been purchased and needs to be registered, the CB obtains its "CB certificate" from the CSS. However, Benussi does not disclose or suggest that the CSS transmits the CB certificate to the CB when a request for encrypted communication is received by the CSS from the CB. On the contrary, Benussi does not disclose or suggest anything remotely similar to the features of the communication device as recited in claims 38 and 44.

Accordingly, for at least the foregoing reasons, Applicants respectfully submit that Smetters and Benussi do not disclose or suggest an image processing apparatus comprising a communication device, which is configured to transmit a second certificate, which includes path information to the first certificate stored in the image forming apparatus, to the client when a connection for encrypted communication is requested by the client after the first certificate stored in the image forming apparatus is installed in the client, as recited in new claims 38 and 44.

New claims 34-37, which depend from claims 1, 7, 17 and 31, respectively, recite features similar to the above-described features of new claims 38 and 44 which are not disclosed or suggested by Smetters and Benussi.

Dependent claims 2, 3, 6, 8, 9, 11, 18, 19, 23, 26, 27, 29, 32 and 33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters and Benussi in view of one or more of Frailong et al. (U.S. Patent No. 5, 012,100, hereinafter "Frailong"), Debry (U.S. Patent No. 5,918,042), Slick (U.S. Patent Application Publication No. 2004/0109568), Vogel et al. (U.S. Patent No. 6,816,900, hereinafter "Vogel"), and Schneier's Applied Cryptography, 2nd Edition (hereinafter "Schneier").

Frailong, Debry, Slick, Vogel and Schneier, either individually or in combination, do not disclose or suggest the features of independent claims 1, 7, 17, 31, 38 and 44 which are not disclosed or suggested by Smetters and Benussi.

Consequently, Frailong, Debry, Slick, Vogel and Schneier cannot cure the deficiencies of Smetters and Benussi for failing to disclose or suggest all the recited features of claims 1, 7, 17, 31, 38 and 44.

Therefore, Applicants respectfully submit that claims 1, 7, 17, 31, 38 and 44, as well as claims 2-6, 8-12, 18-20, 22-24, 28, 29, 32-43 and 44-49 which depend therefrom, are patentable over the applied references, since the applied references, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 7, 17, 31, 38 and 44.

Accordingly, for at least the foregoing reasons, Applicants respectfully submit that claims 1, 7, 17, 31, 38 and 44, as well as claims 2-6, 8-12, 18-20, 22-24, 28, 29, 32-43 and 44-49 which depend therefrom, are patentable over Smetters, Benussi, Frailong, Debry, Slick, Vogel and Schneier.

Dependent claims 2-6, 8-12, 18-20, 22-24, 28, 29, 32-43 and 44-49 recite further distinguishing features over the applied references. The foregoing explanation of the patentability of independent claims 1, 7, 17, 31, 38 and 44 is sufficiently clear such that it is believed to be unnecessary to separately demonstrate the additional patentable features of the dependent claims at this time. However, Applicants reserve the right to do should it become appropriate.

III. Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. Accordingly, a favorable examination and consideration of the instant application are respectfully requested.

If, after reviewing this Amendment, the Examiner believes there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: March 19, 2010

By: /Jonathan R. Bowser/
Jonathan R. Bowser
Registration No. 54574

Customer No. 21839
703 836 6620